To Obtain or not to Obtain CSI in the Presence of Hybrid Adversary

Y. Ozan Basciftci
Dep. of Electrical & Computer Eng.
The Ohio State University
Columbus, Ohio, USA
Email: basciftci.1@osu.edu

C. Emre Koksal
Dep. of Electrical & Computer Eng.
The Ohio State University
Columbus, Ohio, USA
Email: koksal@ece.osu.edu

Fusun Ozguner
Dep. of Electrical & Computer Eng.
The Ohio State University
Columbus, Ohio, USA
Email: ozguner@ece.osu.edu

***Abstract*—We consider the wiretap channel model under the presence of a hybrid, half duplex adversary that is capable of either jamming or eavesdropping at a given time. We analyzed the achievable rates under a variety of scenarios involving different methods for obtaining transmitter CSI. Each method provides a different grade of information, not only to the transmitter on the main channel, but also to the adversary on all channels. Our analysis shows that main CSI is more valuable for the adversary than the jamming CSI in both delay-limited and ergodic scenarios. Similarly, in certain cases under the ergodic scenario, interestingly, no CSI may lead to higher achievable secrecy rates than with CSI.**

I. Introduction

Information theoretic security has received a significant attention recently. One mainstream direction has been on the wireless transmission of confidential messages from a source to a destination, in the presence of internal and/or external eavesdroppers. Toward achieving that goal, the communicating pair exploits the stochasticity and the asymmetry of wireless channels between the communicating pair and the eavesdroppers. A stochastic encoder at the transmitter makes use of the available channel state information (CSI) in a way for the mutual information leaked to the adversaries remain arbitrarily small. It is designed in a way that, even when the adversaries have access to the full CSI of the main channel, i.e., between the transmitter and the receiver as well as the eavesdropper channel, i.e., between the transmitter and itself, it still will obtain an arbitrarily low rate of information on the message. Likewise, the adversary relies on CSI to make decisions. For instance, a half-duplex hybrid adversary, capable of jamming or eavesdropping at a given time (but not both simultaneously) decides between jamming vs. eavesdropping, based on the available CSI.

The assumption that the adversaries have full CSI of all channels is typical in the literature [1]-[3]. While this assumption leads to robust systems in terms of providing security as it makes no assumptions on the adversaries, it can be too conservative in some cases. For example, to obtain main CSI, an adversary relies on the same resource as the transmitter: feedback from the legitimate receiver. Hence, from the perspective of the receiver, there is a tradeoff between revealing CSI and keeping it secret: If the legitimate receiver chooses not to reveal CSI, it will sacrifice some achievable rate of reliable communication, but the adversary will have to make decisions under a higher uncertainty. In this paper, we study the tradeoffs involving obtaining CSI. We ask the questions, should a legitimate pair obtain CSI and if so, what should be their strategy?

To that end, we focus on the system depicted in Figure 1. We assume all three channels to be block fading. In each block, based on the available CSI, the half-duplex adversary can choose to do jamming at a fixed transmission power or eavesdropping, but not both. Our objective is to maximize the rate of reliable communication over the main channel, subject to full equivocation [4] (weak secrecy) at the adversary. The adversary can follow an arbitrary strategy in its choice of jamming vs. eavesdropping at any given block. In the case in which the receiver feeds back main CSI, it may do so in two ways: directly by sending back the exact state of the channel or by sending reverse pilots, trying to exploit channel reciprocity (similar to [5]). While the former method completely reveals the main CSI, it eliminates the possibility of the adversary to learn the jammer CSI. On the other hand, while the pilot feedback successfully hides the main CSI, it enables the adversary to estimate the jammer CSI. In terms of the secrecy encoding strategies, we address the possibilities under two general scenarios: the ergodic and the delay-limited. In the former case, one message is encoded across infinitely many blocks and in the latter case, a separate message is encoded over each block, to be decoded immediately. Thus, in the delay-limited scenario, we also impose an additional probabilistic constraint on the decoding and secrecy outage events.

In the delay limited scenario, we show that by revealing the main CSI, the receiver achieves a higher secrecy rate under the outage constraint, compared to transmission with no CSI. Furthermore, we show that main CSI is more valuable for the adversary than the jamming CSI in both delay-limited and ergodic scenarios. In the ergodic scenario, we observe that the transmitter may not need the CSI to achieve higher secrecy rates.

There is a recent research interest on hybrid adversaris. In [7], the authors formulate the MIMO wiretap channel as a two player zero-sum game in which the payoff function is an achievable ergodic secrecy rate. The strategy of the

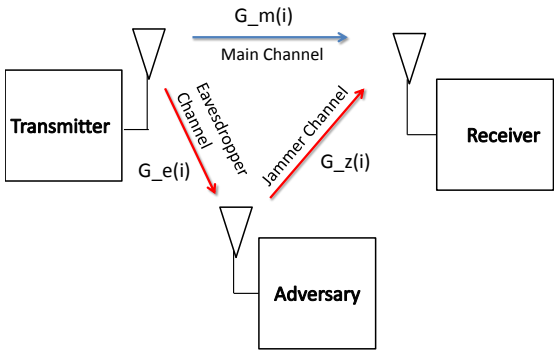

Fig. 1. System Model

transmitter is to send the message in a full power or to utilize some of the available power to produce artificial noise. The conditions under which pure Nash equilibrium exists are studied. In [6], the authors consider fast fading main and eavesdropper channels and static jammer channel. Under this channel configuration, they propose a novel encoding scheme which is called block-Markov Wyner secrey encoding. In [8], the authors introduce a pilot contamination attack in which the adversary jams during the reverse training phase to prevent the transmitter from estimating the main CSI correctly. As a result, the transmitter incorrectly designs precoder which will increase the signal strength at the adversary that eavesdrops the main channel during the data transmission phase.

The rest of this paper is organized as follows. In Section II, we first describe the system model. We then explain the channel model and CSI feedback models. At the end of the section, we explain the problem formulations. In Section III, we present the results for both delay limited and ergodic scenarios. In Section IV, we present our numerical results and conclude the paper in Section V.

II. System Model and Problem Formulation

A. Channel Model

In this paper, we focus on a block fading channel model. Time is divided into discrete blocks and there are N channel uses in each block. Channel state is assumed to be constant within a block and varies randomly from one block to the next. We assume all parties are half-duplex, thus the adversary can not jam and eavesdrop simultaneously.

The observed signals at the legitimate receiver and the adversary in i-th block are as follows:

$$Y^N(i) = G_m(i)X^N(i) + G_z(i)S_j^N(i)I_J(i) + S_m^N(i) \quad (1)$$

$$Z^N(i) = G_e(i)X^N(i)(1 - I_J(i)) + S_e^N(i) \quad (2)$$

where $X^N(i)$ is the transmitted signal, P is the transmission power, $Y^N(i)$ is the signal received by the legitimate receiver, $Z^N(i)$ is the signal received by the adversary, $S_j^N(i)$, $S_m^N(i)$, and $S_e^N(i)$ are noise vectors distributed as complex Gaussian, $\mathcal{CN}(\mathbf{0}, P_j I_{N\times N})$, $\mathcal{CN}(\mathbf{0}, I_{N\times N})$, and $\mathcal{CN}(\mathbf{0}, I_{N\times N})$, respectively, and P_j is the jamming power. Indicator function $I_J(i) = 1$, if the adversary is in a jamming state in the i-th block; otherwise $I_J(i) = 0$. Channel gains, $G_m(i)$, $G_e(i)$, and $G_z(i)$ are defined to be the independent complex gains of transmitter-to-receiver channel, transmitter-to-adversary channel, and adversary-to-receiver channel, respectively (as illustrated in Figure 1). Associated power gains are denoted with $H_m(i) = |G_m(i)|^2$, $H_e(i) = |G_e(i)|^2$, and $H_z(i) = |G_z(i)|^2$. We assume that channel reciprocity principle is valid for all channels, i.e., reverse channels and forward channels have identical gains. We also assume that joint probability density function of instantaneous power gains, $f_{\mathbf{H}}(\mathbf{h})$, where $\mathbf{H} = [H_m(\cdot)\ H_e(\cdot)\ H_z(\cdot)]$, is well defined and known by all entities.

B. Methods for Obtaining CSI

The legitimate pair may choose to obtain main CSI or communicate without it. We call the latter strategy the *no CSI case*. If they choose to obtain main CSI, at the beginning of each time block, the transmitter sends training symbols to the legitimate receiver. In this paper, we ignore the overhead associated with this training process. We assume that, using the training symbols sent at the beginning of block i, the legitimate receiver obtains perfect knowledge of $G_m(i)$ and the adversary obtains perfect knowledge of $G_e(i)$.

Once the receiver observes main CSI, it uses two possible methods for feeding back this information. The first one is directly feeding back the observed channel state: the value of $G_m(i)$ is encoded at the receiver and sent to the transmitter in a feedback packet. Thus, we call this feedback method the *packet feedback*. We assume that the legitimate receiver and the adversary both decode this packet successfully and learn $G_m(i)$. The second method is using pilot based CSI feedback in which the receiver sends training symbols to the transmitter. We call this second method the *pilot feedback*. We assume that by using these reverse training symbols, the legitimate transmitter obtains perfect knowledge of $G_m(i)$ and the adversary obtains the perfect knowledge of $G_z(i)$. Thus, in the first method, the adversary obtains the knowledge of $G_m(i)$, but not $G_z(i)$, whereas the reverse is true in the second method.

C. Adversary Model

The goal of the adversary is to minimize the achieved secrecy rate. The strategy space of the adversary in each block is binary: jamming or eavesdropping. The transmitter does not observe the strategy of the adversary in any given block, whereas we assume that the adversary knows the strategy of the transmitter a priori.

From one block to the next, the adversary chooses its strategy based on the transmitter's strategy and the obtained channel power gains[1], i.e., $h_e(i)$ for the no CSI case, $h_e(i)$, $h_m(i)$ for the packet feedback case, and $h_e(i)$, $h_z(i)$ for the pilot feedback case. We denote the vector of channel power

[1]The realizations of the random variables are represented by lower case letters in the sequel.

gains observed by the adversary at the beginning of the ith block with $\mathbf{h}_A(i)$.

The secrecy level of a transmitted message is measured by the equivocation rate at the adversary. The equivocation rate at the adversary is defined as the entropy of the transmitted message conditioned on the channel output and the available CSI at the adversary. If the equivocation rate is equal to the secrecy rate, the message is said to be transmitted with *perfect secrecy*.

D. Encoding of Information

In our system, we consider two levels of encoding. At the higher level, secrecy is realized Wyner code introduced in [4]. There, $C_s(R_m, R_s, NM)$ represents a Wyner code of size 2^{NMR_m} that bears a confidential message set $W_s = \{1, 2, \ldots, 2^{NMR_s}\}$, where NM is the codeword length in number of bits. A message, $w_s \in W_s$ is mapped to NMR_m bits by a secrecy encoder [4] and these NMR_m bits are then mapped to channel encoded bits at the lower level of encoding using a sequence of codes, $C_i(2^{NR(h_m(i))}, N)$, one for each block i, $1 \leq i \leq M$. Here, the code rate, $R(h_m(i))$, is chosen based on the main CSI, obtained at the transmitter. The sequence of codewords is denoted with $x^{NM} \in \mathcal{X}^{NM}$, and the decoder, $\phi(\cdot)$ maps the received sequence, Y^{NM} to $\hat{w} \in \mathcal{W}$. The average error probability of the sequence of codes $\{C_i\}$ is denoted with the associated sequence P_e^{NM}. In this paper, we focus on two scenarios as to how secrecy encoding and channel encoding are applied: delay limited and ergodic.

1) Delay-Limited Scenario: In the delay-limited scenario, the transmitter encodes a separate secret message, $W_s(i)$ in each block i. Consequently, we use a separate secrecy encoder $C_s(i) = C_s(R_m(i), R_s, N)$ for each block, where $R_m(i)$ is chosen to be identical to $R(h_m(i))$ to meet the channel rate. The channel encoder merely maps these $NR_m(i)$ bits to N Gaussian random variables, X^N, forming a Gaussian codebook $C_i(2^{NR(h_m(i)}, N)$. For the delay-limited scenario, we define the secrecy outage and connection outage events [3] as:

$$\frac{I(X^N; Z^N|h_e(i))}{N} > R(h_m(i)) - R_s \quad \text{and} \tag{3}$$

$$\frac{I(X^N; Y^N|h_m(i))}{N} < R(h_m(i)), \tag{4}$$

respectively, where $X^N \sim \mathcal{CN}(\mathbf{0}, PI_{N\times N})$

2) Ergodic Scenario: In the ergodic scenario, the transmitter has one secret message W_s and encodes it over M blocks using the $C_s(R_m, R_s, NM)$ encoder. In the ergodic scenario, secrecy rate R_s is said to be achievable if, for any $\epsilon > 0$, there exists sequence of channel codes $\{C_i\}$ for which the following are satisfied:

$$P_e^{NM} \leq \epsilon \tag{5}$$

$$\frac{1}{MN} H(W_s|Z^{MN}, \mathbf{h}_A^M) \geq R_s - \epsilon \tag{6}$$

for sufficiently large N and M and for any $\mathbf{h}_A^M \in \mathcal{A}_M$ such that $P[\mathcal{A}_M] = 1$. Here, we consider two possible channel encoding strategies:

1. Encoding across blocks: We use this strategy in the no main CSI case. In this strategy, the NMR_m bits at the output of the secrecy encoder is channel encoded via a single $C(2^{NMR_m}, NM)$ Gaussian codebook and the NM symbols are transmitted over the channel over M blocks.

2. Block-by-block encoding: We use this strategy when the main CSI is available. To utilize the main channel knowledge, the transmitter chooses some h_z^* and encodes the information using a Gaussian codebook with the rate $R(h_m(i)) = \log\left(1 + \frac{Ph_m(i)}{1+P_j h_z^*}\right)$ over block i. With this choice, the transmitted codeword will not be decoded successfully if the adversary is in the jamming state and $h_z(i) > h_z^*$. To handle this possibility, we use a plain ARQ strategy in each block (similar to [9]). Transmissions that receive a negative acknowledgement (NAK) are retransmitted until they are decoded successfully.

E. Problem Formulation

One can notice that, in both the delay-limited and the ergodic scenarios, we use a constant secrecy rate[2] R_s. The goal of the transmitter is to maximize the secrecy rate, R_s over the strategy space of secrecy encoding and channel encoding rates. To that end, we consider the worst case scenario, in which the adversary perfectly tracks the strategy of the transmitter in each block. Furthermore, since the transmitter does not know the real state of the adversary, the strategy pair of the transmitter should satisfy the constraint for any arbitrary strategy of the adversary. Thus, we choose the secrecy rate using:

$$R_s^* = \max_{R_m(i), R_s} \min_{I_J(i)} R_s \tag{7}$$

for all i in both the delay-limited and the ergodic scenarios, subject to the following outage constraint in the delay-limited scenario only:

$$\lim_{M\to\infty} \frac{1}{M} \sum_{i=1}^{M} I_J(i) I_C(i) + (1 - I_J(i)) I_S(i) I_C(i) \geq \alpha \tag{8}$$

with probability 1, where $I_C(i)$ and $I_S(i)$ are indicator functions that take on a value 0 in case of a connection and a secrecy outage, respectively. We evaluate R_s^* under the no CSI, packet feedback, and pilot feedback cases. Note that the constraint enforces that the fraction of packets that are not in the both secrecy outage and the connection outage should be larger than a threshold as the number of blocks, M, goes to infinity.

Note that, the reason why we focus on the specific encoding strategies specified under delay limited and ergodic scenarios in Section II-D is that, the solution, R_S^*, of the maximin problem stated in (7) is unknown [11].

[2]For the delay-limited case, it is constant over the entire sequence of Wyner codes.

III. Results

A. Delay Limited Scenario

The outage constraint in (8) is formulated as

$$C = \lim_{M\to\infty} \frac{1}{M}\sum_{i=1}^{M} I_J(i) I_{\log\left(1+\frac{PH_m(i)}{1+P_jH_z(i)}\right)\geq R(H_m(i))} + (1-I_J(i)) I_{\log(1+PH_e(i))\leq R(H_m(i))-R_s} \times I_{\log(1+PH_m(i))\geq R(H_m(i))} \quad (9)$$

Note that in (9), the secrecy outage event is represented with $\log(1+Ph_e(i)) > R(h_m(i)) - R_s$ and the connection outage events are given as $\log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right) < R(h_m(i))$ and $\log(1+Ph_m(i)) < R(h_m(i))$.

Theorem 1. *For the delay limited scenario, the solution of (7), subject to constraint (9) leads to the following ordering of the achievable rate with respect to the type of feedback:*

$$R_s^{\text{No CSI}} \leq R_s^{\text{Packet feedback}} \leq R_s^{\text{Pilot Feedback}} \quad (10)$$

The above theorem implies that main CSI, which is obtained with packet feedback is more valuable for the adversary than the jammer CSI, which is obtained with pilot feedback. We now give an outline for the proof. The details of the proof can be found in Section VI.

The Outline of Proof of Theorem 1: The basic idea is to compare the feasible set of the problem (7) for three cases. The feasible set is defined as

$$\mathcal{F} = \{(R_s, R(\cdot)) : C \geq \alpha \text{ w.p. } 1, \forall A_p\} \quad (11)$$

where A_p is the set of channel power gains, $h_A(i)$, such that the adversary is in the jamming state if $h_A(i) \in A_p$. The equivalent form of (7) is as follows: $R_s^* = \max_{(R_s,R(\cdot))\in\mathcal{F}} R_s$. We observe that the solution to (7) is directly related to the size of the feasible set. The strategy pair $(R_s, R(\cdot))$ is the element of the feasible set, $\mathcal{F}$ if $C_{\min} = \min_{A_p} C[(R_s, R(\cdot))] \geq \alpha$ w.p. 1. We can write $C_{\min}$ for the no CSI and packet feedback cases as follows:

$$C_{min}^{\text{Packet Feedback}} = P\left[R_s + \log(1+PH_e) \leq R(H_m) \leq \log\left(1+\frac{PH_m}{1+P_jH_z}\right)\right]$$

$$C_{min}^{\text{No CSI}} = P\left[R_s + \log(1+PH_e) \leq R \leq \log\left(1+\frac{PH_m}{1+P_jH_z}\right)\right]$$

We can observe that $F^{\text{No CSI}} \subset F^{\text{Packet Feedback}}$ so we have $R_s^{\text{No CSI}} \leq R_s^{\text{Packet feedback}}$. By assuming the adversary is full-duplex, we find a lower bound, $C^{\text{lower bound}}$ for C_{min} at CSI feedback cases. Then, we observe $C^{\text{lower bound}} = C_{min}^{\text{Packet Feedback}}$ which shows $C_{min}^{\text{Packet Feedback}} \leq C_{min}^{\text{Pilot Feedback}}$ and this concludes the proof. ■

B. Ergodic Scenario

We first present a secrecy rate that is achievable under the no CSI case.

Theorem 2. *The achieved secrecy under no CSI is:*

$$R_s^{\text{No CSI}} = \left[\mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right) - \log(1+PH_e)\right]\right]^+ \quad (12)$$

The proof of (12) can be found at Section VII. Next, we present an upper bound for the secrecy rates achieved with the block-by-block encoding strategy.

Theorem 3. *Under the block-by-block encoding strategy, the achievable secrecy rate is upper bounded by*

$$R_s^+ = \mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right) - \log(1+PH_e)\right]^+ \times P[H_z \leq h_z^*] \quad (13)$$

To find this upper bound, we employ the following strategy. When the transmitter receives a NAK signal, the transmitter sends an independent group of bits on the next block instead of retransmitting the previous packet [12]. In [12], the authors use this scheme for the secret key sharing. The crucial observation is that an upper bound for the achievable secret key rate is also an upper bound for the achievable secrecy rates. The details of the proof can be found at Section VIII. Note that with the plain ARQ strategy described in Section II-D2, the achievable rate is identical to the expression provided in (13), with $P[H_z \leq h_z^*]$ replaced with $(P[H_z \leq h_z^*])^2$, and H_z in the expectation term replaced with h_z^* as shown in [9].

By comparing the upper bound given in Theorem 3, we gain understanding on the performance of no CSI case. In particular, whenever the achievable rate with the no CSI case exceeds this bound, we know for sure that encoding across blocks (no CSI) is preferable over block-by-block encoding with CSI. The main difference between block-by-block encoding and encoding across blocks is that, in the former, the unsuccessfully received packets are discarded, whereas in the no CSI case, all the information received by the receiver is used to decode the message. The set of parameters for which this is the case is illustrated in Section IV in an example.

One can also write a general relationship between the performance with packet feedback and pilot feedback:

Theorem 4. *Any secrecy rate achievable with packet feedback strategy is also achievable with pilot feedback strategy.*

Theorem 4, shows that main CSI is more valuable for the adversary than the jamming CSI in the ergodic scenario, as was the case in the delay limited scenario. The proof can be found at Section IX

IV. Numerical Evaluation

We first analyze the delay-limited case. We assume that both main and eavesdropper channels are characterized by block Rayleigh fading, where the main channel and eavesdropper

channel power gains follow an exponential distribution with a mean 10 and 1, respectively[3]. We also assume the jamming channel does not experience fading, where power gain is equal to 1. The transmission power, P, and the jamming power, P_j are identical and chosen to be 1. In Figure 2, we plot the secrecy rate, R_s, as a function of the outage constraint threshold, α under the no CSI, the packet feedback, and the pilot feedback cases. The achievable rates in Figure 3 follow the same ordering as given in Theorem (1).

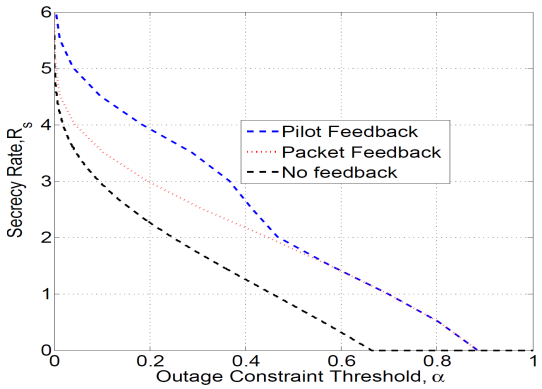

Fig. 2. Delay Limited Scenario: Comparison of CSI feedback methods under the outage constraint.

Next, we simulate the ergodic scenario and compare the two strategies, encoding across blocks without CSI and block-by-block encoding with packet CSI feedback. We used the same power parameters as in the simulations for the delay-limited case. All three channels are assumed to be block Rayleigh-fading wtih $E[H_z] = 1$ We select the encoding parameter, h_z^* such that $P[H_z \leq h_z^*] = 0.75$.

In Figure 3, we illustrate the region where the encoding across blocks outperforms the block-by-block encoding on the $(E[H_e], E[H_m])$ space. The region to the left of the border, given in the plot contains the set of $(E[H_e], E[H_m])$ for which the encoding across blocks results in a higher secrecy rate. The intuition behind this observation is that, when $E[H_m]$ is much larger than $E[H_e]$, the positive operator inside the upper bound, R^+ loses its significance.

V. Conclusion

We consider the wiretap channel model under the presence of half duplex adversary that is capable of either jamming or eavesdropping at a given time. We analyzed the achievable rates under a variety of scenarios involving different methods for obtaining transmitter CSI. In particular, we considered no CSI, CSI with packet based feedback, and CSI with pilot based feedback. Each method provides a different grade of information not only to the transmitter on the main channel, but also to the adversary on all channels. We show for the

[3]Such a difference may occur in the cellular setting, when the receiver is a base station with many antennas or in a wireless LAN setting, where the receiver is located at a favorable position for reception, compared to an external adversary.

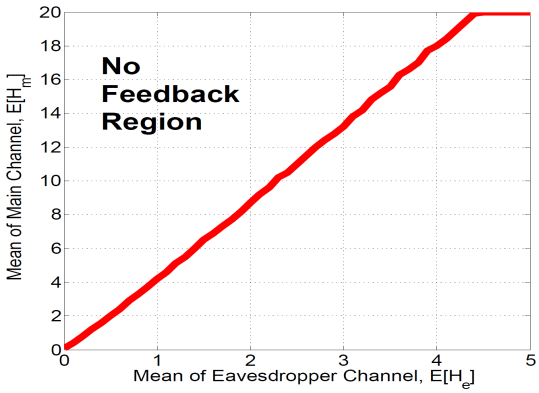

Fig. 3. The region where encoding across blocks with no CSI outperforms block-by-block encoding with packet feedback.

delay limited scenario that, the highest secrecy rate is achieved with the pilot based feedback. Similarly, in the ergodic case, we prove that the pilot-based CSI feedback outperforms the packet-based CSI feedback, however interestingly, in certain cases no CSI may lead to a higher achievable secrecy rates than with CSI.

VI. Proof of Theorem 1

Feasible set for the problem (7) is defined to be

$$\mathcal{F} = \{(R_s, R(\cdot)) : C \geq \alpha, \forall A_p\} \tag{14}$$

where A_p is the set of channel power gains such that the adversary is in the jamming state if $h_A(i) \in A_p$. We have the following lemma.

Lemma 5. *If $\mathcal{F} \neq \emptyset$, the solution to (7) is identical for all strategies of the adversary.*

Proof: The equivalent form of (7) is as follows:

$$R_s^* = \max_{(R_s, R(\cdot)) \in \mathcal{F}} R_s \tag{15}$$

As seen from (15), R_s^* does not depend on strategy of the adversary. ■

However, the size of feasible set directly depends on the CSI feedback scheme. From (15), we can see that the solution to (7) is directly proportional with the size of the feasible set. In the rest of the proof, we will use this observation to show the ordering.

Lemma 6. $R_s^{\textit{No CSI}} \leq R_s^{\textit{Packet Feedback}}$

Proof: In the no feedback case, constraint term (9) is reduced to

$$\begin{aligned} C &= \lim_{M\to\infty} 1/M \sum_{i=1}^{M} I_J(i) I_{\log\left(1+\frac{PH_m(i)}{1+P_j H_z(i)}\right)\geq R} \\ &+ (1 - I_J(i)) I_{\log(1+PH_e(i))\leq R-R_s} I_{\log(1+PH_m(i))\geq R} \\ &= \lim_{M\to\infty} 1/M \sum_{i=1}^{M} I_{H_e(i)\in A_p} I_{\log\left(1+\frac{PH_m(i)}{1+P_j H_z(i)}\right)\geq R} \end{aligned} \tag{16}$$

$$+ I_{H_e(i)\notin A_p} I_{\log(1+PH_e(i))\le R-R_s} I_{\log(1+PH_m(i))\ge R} \quad (17)$$

$$= E\left[I_{H_e\in A_p} I_{\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\ge R} \right.$$
$$\left. + I_{H_e\notin A_p} I_{\log(1+PH_e)\le R-R_s} I_{\log(1+PH_m)\ge R} \right], \text{ w.p. } 1 \quad (18)$$

$$= \int_{h_e} E\left[I_{\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\ge R} I_{H_e\in A_p} \right.$$
$$\left. + I_{\log(1+PH_e)\le R-R_s} I_{\log(1+PH_m)\ge R} I_{H_e\notin A_p} \mid H_e = h_e \right]$$
$$f_{H_e}(h_e)\, dh_e, \text{ w.p. } 1 \quad (19)$$

$$= \int_{h_e} E\left[I_{\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\ge R} \right] I_{h_e\in A_p}$$
$$+ E[I_{\log(1+PH_m)\ge R}] I_{\log(1+Ph_e)\le R-R_s} I_{h_e\notin A_p}$$
$$f_{H_e}(h_e)\, dh_e, \text{ w.p. } 1 \quad (20)$$

where (17) follows from the fact that we have $I_J(i) = I_{H_e(i)\in A_p}$ since the adversary only knows the instantaneous power gain of the eavesdropper channel, (18) follows from the strong law of large numbers theorem and (20) follows from the independence of H_e, H_m, and H_z.

A_p^* set that minimizes C is as follows:

$$A_p^* = \{h_e \ : \log(1+Ph_e) \le R - R_s\} \quad (21)$$

The minimized C for a given rate pair (R_s, R) is

$$C^{\text{No CSI}} =$$
$$\mathbf{P}\left[R_s + \log(1+PH_e) \le R \le \log\left(1+\frac{PH_m}{1+P_jH_z}\right) \right]$$

Feasible set for the transmitter for the no CSI feedback case is as follows

$$F^{\text{No CSI}} = \{(R_s, R) \ : C^{\text{No CSI}} \ge \alpha\} \quad (22)$$

We now show that $F^{\text{No CSI}} \subset F^{\text{Packet Feedback}}$. For the packet feedback case, channel encoding rate is a function of the main CSI, H_m. The adversary knows the instantaneous power gains of the eavesdropping channel and the main channel. Constraint term in (9) is reduced to

$$C = \lim_{M\to\infty} 1/M \sum_{i=1}^{M} I_J(i) I_{\log\left(1+\frac{PH_m(i)}{1+P_jH_z(i)}\right)\ge R(H_m(i))}$$
$$+ (1-I_J(i)) I_{\log(1+PH_e(i))\le R(H_m(i))-R_s}$$
$$I_{\log(1+PH_m(i))\ge R(H_m(i))} \quad (23)$$

$$= \lim_{M\to\infty} 1/M \sum_{i=1}^{M} I_{(H_m(i),H_e(i))\in A_p} I_{\log\left(1+\frac{PH_m(i)}{1+P_jH_z(i)}\right)\ge R(H_m(i))}$$
$$+ I_{(H_m(i),H_e(i))\notin A_p} I_{\log(1+PH_e(i))\le R(H_m(i))-R_s}$$
$$I_{\log(1+PH_m(i))\ge R(H_m(i))} \quad (24)$$

$$= E\left[I_{H_m,H_e\in A_p} I_{\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\ge R(H_m)} \right.$$
$$\left. + I_{H_m,H_e\notin A_p} I_{\log(1+PH_e)\le R(H_m)-R_s} I_{\log(1+PH_m)\ge R} \right], \text{ w.p. } 1 \quad (25)$$

$$= \int_{h_m,h_e} E\left[I_{\log\left(1+\frac{Ph_m}{1+P_jH_z}\right)\ge R(h_m)} \right] I_{h_m,h_e\in A_p}$$
$$+ I_{\log(1+Ph_e)\le R(h_m)-R_s} I_{\log(1+Ph_m)\ge R(h_m)} I_{h_m,h_e\notin A_p}$$
$$f_{H_e}(h_e) f_{H_m}(h_m)\, dh_e dh_m, \text{ w.p. } 1 \quad (26)$$

where (24) follows from the facet that $I_J(i) = I_{H_m(i),H_e(i)\in A_p}$ since the adversary knows both the instantaneous power gain of the eavesdropper channel and the main channel. (25) follows from the strong law of large numbers theorem and (26) follows from the independence of H_e, H_m, and H_z. A_p^* set that minimizes C is as follows:

$$A_p^* = \{h_m, h_e \ : \log(1+Ph_e) \le R(h_m) - R_s\}$$
$$\bigcup \{h_m, h_e \ : \log(1+Ph_m) \le R(h_m)\} \quad (27)$$

When we combine (26) and (27), the minimized can be $C^{\text{Packet Feedback}}$ written as

$$C^{\text{Packet Feedback}} =$$
$$P\left[R_s + \log(1+PH_e) \le R(H_m) \le \log\left(1+\frac{PH_m}{1+P_jH_z}\right) \right].$$

Feasible set for the transmitter for the packet feedback case is as follows

$$F^{\text{Packet Feedback}} = \{(R_s, R(\cdot)) \ : C^{\text{Packet Feedback}} \ge \alpha\} \quad (28)$$

It is easy to see that $F^{\text{No CSI}} \subset F^{\text{Packet Feedback}}$ then we have $R_s^{\text{No CSI}} \le R_s^{\text{Packet Feedback}}$. ■

Lemma 7. $R_s^{\textit{Packet Feedback}} \le R_s^{\textit{Pilot Feedback}}$

Proof: We will show that for any given $(R_s, R(\cdot))$, $C^{\text{Packet Feedback}}$ is a lower bound for (9) in the channel feedback cases. Constraint (9) can be written as

$$C = \lim_{M\to\infty} 1/M \sum_{i=1}^{M} \left[1 - I_{H_m(i),H_e(i),H_z(i)\in\mathcal{O}}\right] \quad (29)$$

where

$$\mathcal{O} = \{h_m(i), h_e(i), h_z(i) : I_J(i) I_{\log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right)\le R(h_m(i))} = 1\}$$
$$\bigcup \{h_m(i), h_e(i), h_z(i) : I_E(i) I_{\log(1+Ph_e(i))\ge R(h_m(i))-R_s} = 1\}$$
$$\bigcup \{h_m(i), h_e(i), h_z(i) : I_E(i) I_{\log(1+Ph_m(i))\le R(h_m(i))} = 1\} \quad (30)$$

Constraint C decreases as the siz of set $\mathcal{O}$ increases. Let's define an upper bound for $\mathcal{O}$:

$$\mathcal{O}^{\text{Upper Bound}}$$
$$= \{h_m(i), h_e(i), h_z(i) : I_{\log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right)\le R(h_m(i))} = 1\}$$
$$\bigcup \{h_m(i), h_e(i), h_z(i) : I_{\log(1+Ph_e(i))\ge R(h_m(i))-R_s} = 1\}$$
$$\bigcup \{h_m(i), h_e(i), h_z(i) : I_{\log(1+Ph_m(i))\le R(h_m(i))} = 1\} \quad (31)$$

where $I_J(i) = I_E(i) = 1, \forall i \in \mathbb{N}$. Then, we find a lower bound for C by putting $\mathcal{O}^{\text{Upper Bound}}$ in (29):

$$C^{\text{Lower Bound}}$$

$$= \lim_{M\to\infty} \sum_{i=1}^{M} I_{\log\left(1+\frac{PH_m(i)}{1+P_jH_z(i)}\right)\geq R(H_m(i))\geq \log(1+PH_e(i))+R_s}$$
$$= C^{\text{Packet CSI}} \tag{32}$$

Since $C^{\text{Lower Bound}} = C^{\text{Packet Feedback}}$, we have $\mathcal{F}^{\text{Lower Bound}} = \mathcal{F}^{\text{Packet Feedback}} \subset \mathcal{F}^{\text{Pilot Feedback}}$. ∎

VII. Proof of Theorem 2

We employ the *encoding across block* strategy explained in Section II-D, where $R_m \triangleq \mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\right]$. If $R_m < \mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\right]$, the adversary prevents the reliable communication by jamming at every block. Note that in no CSI case, the adversary only obtains $h_e(i)$ so equivocation rate is defined as $\frac{H(W|Z^{NM},h_e^M)}{NM}$. Equivocation analysis for the *encoding across block* is as follows.

$$\begin{aligned}
&H(W|Z^{NM},h_e^M)\\
&= H(W,X^{NM}|Z^{NM},h_e^M) - H(X^{NM}|Z^{NM},W,h_e^M)\\
&= H(X^{NM}|Z^{NM},h_e^M) + H(W|X^{NM},Z^{NM},h_e^M)\\
&\qquad - H(X^{NM}|Z^{NM},W,h_e^M)\\
&\geq H(X^{NM}|Z^{NM},h_e^M) + H(X^{NM}|Z^{NM},W,h_e^M)\\
&= H(X^{NM}|h_e^M) - I(X^{NM},Z^{NM}|h_e^M)\\
&\qquad + H(X^{NM}|Z^{NM},W,h_e^M)\\
&\overset{(a)}{=} MNR_m - I(X^{NM},Z^{NM}|h_e^M)\\
&\qquad - H(X^{NM}|Z^{NM},W,h_e^M)\\
&\geq MNR_m - N\sum_{i=1}^{M} I(X^N(i),Z^N(i)|h_e(i))\\
&\qquad - H(X^{NM}|Z^{NM},W,h_e^M)\\
&\geq MNR_m - N\sum_{i=1}^{M} \log(1+Ph_e(i))\\
&\qquad - H(X^{NM}|Z^{NM},W,h_e^M)
\end{aligned}$$

where (a) follows from the fact that codeword X^{NM} is uniformly distributed over a set of size 2^{NMR_m}. We continue with the following steps.

$$\begin{aligned}
&\frac{H(W|Z^{NM},h_e^M)}{NM}\\
&\geq R_m - \frac{\sum_{i=1}^{M}\log(1+Ph_e(i))}{M} - \frac{H(X^{NM}|Z^{NM},W,h_e^M)}{NM}\\
&\overset{(b)}{\geq} R_m - E\left[\log(1+PH_e)\right] - \epsilon_1\\
&\qquad - \frac{H(X^{NM}|Z^{NM},W,h_e^M)}{NM},\\
&\overset{(c)}{\geq} R_m - E\left[\log(1+PH_e)\right] - \epsilon_1 - \epsilon_2\\
&= R_s - \epsilon,
\end{aligned}$$

where $\epsilon = \epsilon_1 + \epsilon_2$. Here, (b) is satisfied for any $\epsilon_1 > 0$ and $h_e^M \in A_M$ with $Pr[A_M] = 1$ and $M \geq M(\epsilon_1)$ since

$$\lim_{M\to\infty}\frac{1}{M}\sum_{i=1}^{M}\log(1+PH_e(i)) = E\left[\log(1+PH_e)\right]$$

with probability 1, (c) follows from the Fano's inequality. Let's define $R_e \triangleq R_m - R_s$ and $P_e^{NM} \triangleq P[X^{NM} \neq \hat{X}^{NM}]$ where $\hat{X}^{NM} = g(Z^{NM},h_e^M,W)$ is the estimation of the codeword X^{NM}.

$$\frac{H(X^{NM}|Z^{NM},W,h_e^M)}{NM} \leq P_e^{NM}R_e + \frac{H(P_e^{NM})}{NM} \tag{33}$$
$$\leq \epsilon_2 \tag{34}$$

Here, any $\epsilon_2 > 0$, (34) is satisfied for sufficiently high N and M. The reason is that since $R_e = I(X^N,Z^N|H_e)$, $P_e^{NM} \to 0$ for the sequence of codes $(2^{NMR_e},R_e)$ as $M\to\infty$.

VIII. Proof of Theorem 3

We first show that if R_s is an achievable secrecy rate under the packet feedback strategy, we have for any $\epsilon > 0$, $\frac{1}{NM}H(W|Z^{NM},H_m^M,H_e^M) \geq R_s - \epsilon, \forall N \geq N(\epsilon), \forall M \geq M(\epsilon)$. Note that here, the message W is conditioned on random vectors, H_e^M and H_m^M.

$$\frac{1}{NM}H(W|Z^NM,H_m^M,H_e^M) \tag{35}$$
$$= \int_{\mathcal{A}_M}\frac{1}{NM}H(W|Z^NM,h_M^M,h_e^M)f_{H_m^M,H_e^M}(h_m^M,h_e^M)\,dh_m^M\,dh_e^M$$
$$\geq \int_{\mathcal{A}_M}(R_s-\epsilon)f_{H_m^M,H_e^M}(h_m^M,h_e^M)\,dh_m^M\,dh_e^M \tag{36}$$
$$= R_s - \epsilon \tag{37}$$

where $\mathcal{A}_M$ is the set defined in Section II-D2. Here, (36) follows from the definition of achievability, and (37)follows from the fact that $P[\mathcal{A}_M] = 1$. We consider the following case for the rest of the proof. When the transmitter receives a NACK signal, on the next block, the transmitter sends an independent group of bits instead of retransmitting the previous packet [12]. In [12], the authors use this scheme for the secret key sharing. The crucial observation is that an upper bound for an achievable secret key rate is also an upper bound for achievable secrecy rates.

We define index set F that contains the indexes of blocks on which the transmitted codeword is successfully decoded. Suppose that size of F is M', $n' \triangleq NM'$, and $n \triangleq NM$. We now prove that $\frac{1}{n}H(W|Z^n,H_m^M,H_e^M) \leq R_s^+$ as $n\to\infty$.

$$\begin{aligned}
&H(W|Z^n,H_m^M,H_e^M)\\
&\overset{(a)}{\leq} H(W|Z^n,H_m^M,H_e^M)\\
&\quad - H(W|Z^n,Y^n,H_m^M,H_z^M,H_e^M) + n\delta_n\\
&\overset{(b)}{=} H(W|Z^{n'},H_m^{M'},H_e^{M'})\\
&\quad - H(W|Z^{n'},Y^{n'},H_m^{M'},H_z^{M'},H_e^{M'}) + n\delta_n\\
&= I(W;Y^{n'},H_z^{n'}|Z^{n'},H_m^{M'},H_e^{M'}) + \delta_n
\end{aligned}$$

$$\stackrel{(c)}{\leq} I(X^{n'};Y^{n'},H_z^{M'}|Z^{n'},H_m^{M'},H_e^{M'})+\delta_n$$
$$= I(X^{n'};H_z^{M'}|Z^{n'},H_m^{M'},H_e^{M'}) + I(X^{n'};Y^{n'}|Z^{n'},H_m^{M'},H_e^{M'},H_z^{M'})+n\delta_n$$
$$\stackrel{(d)}{=} I(X^{n'};Y^{n'}|Z^{n'},H_m^{M'},H_e^{M'},H_z^{M'})$$
$$\stackrel{(e)}{=} \sum_{i=1}^{M} I(X^N(i);Y^N(i)|Z^N(i),H_z(i),H_m(i),H_e(i))I(i) + n\delta_n$$
$$\stackrel{(f)}{\leq} \sum_{i=1}^{M} N\mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right)-\log(1+PH_e)\right]^+ I(i) + n\delta_n$$

where $I(i) = I_{H_z(i)\leq h_z^*}$. Here, (a) follows from Fano's inequality (b) follows from the independent choice of the codeword symbols transmitted in each block that does not allow the eavesdropper to benefit from the observations corresponding to the previous NACKed blocks, (c) results from the data processing inequality, (d) follows from the independence of $X^{n'}$ and $H_z^{M'}$, (e) follows from [2], and (f) follows from [10].

$$\frac{1}{n}H(W|Z^n,H_m^M,H_e^M) \tag{38}$$
$$\leq \mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right)-\log(1+PH_e)\right]^+ \times \frac{1}{M}\sum_{i=1}^{M}\mathbf{I}(\mathbf{i})+\delta_n \tag{39}$$
$$R_e \stackrel{(g)}{\leq} \alpha\mathbf{E}\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right)-\log(1+PH_e)\right]^+$$

(g) follows from the fact that $\delta_n \to 0$ as $N, M \to \infty$ and from the ergodicity of channels such that $\frac{1}{M}\sum_{i=1}^{M} I(i) \to P[H_z \leq h_z^*]$ as $M \to \infty$.

IX. Proof of Theorem 4

Suppose that R_s is a secrecy rate achieved with the packet based strategy and $n \triangleq NM$. Notice that the equivocation rates for the pilot and packet feedbacks are defined as $\frac{1}{n}H(W|Z^n,h_e^M)$ and $\frac{1}{n}H(W|Z^n,h_e^M,h_m^M)$, respectively. Since R_s is an achievable rate with the packet based strategy, by definition, for any $\epsilon > 0$ there exists $N(\epsilon)$ and $M(\epsilon)$ such that for $N \geq N(\epsilon)$ and $M \geq M(\epsilon)$, we have $\frac{1}{n}H(W|Z^n,h_e^M,h_m^M) \geq R_s - \epsilon$, $\forall (h_e^M,h_m^M) \in \mathcal{A}_M$ with $P(\mathcal{A}_M)=1$.

We define $\mathcal{A}_M(h_e^M) = \{h_m^M : (h_m^M,h_e^M) \in \mathcal{A}_M\}$. Since H_m^M and H_e^M are independent random vectors and $P[(H_m^M,H_e^M)\in\mathcal{A}_M]=1$, we have $P[H_m^M \in \mathcal{A}_M(h_e^M)] = 1, \forall h_e^M \in \mathcal{A}_M$. To observe that

$$1 = \int_{\mathcal{A}_M} f_{H_m^M,H_e^M}(h_m^M,h_e^M)\,dh_m^M\,dh_e^M \tag{40}$$
$$= \int_{h_e^M} f_{H_e^M}(h_e^M)\int_{h_m^M\mathcal{A}_M(h_e^M)} f_{H_m^M}(h_m^M)\,dh_m^M\,dh_e^M \tag{41}$$
$$= \int_{h_e^M} P[H_m \in \mathcal{A}_M(h_e^M)] f_{H_e^M}(h_e^M)\,dh_e^M = 1 \tag{42}$$

We can see that $P[H_m \in \mathcal{A}_M(h_e^M)] = 1$, $\forall h_e^M \in \mathcal{E}$ such that $P[\mathcal{E}] = 1$. We now prove the lemma with following inequalities.

$$\frac{1}{n}H(W|Z^n,h_e^M) \stackrel{(a)}{\geq} \frac{1}{n}H(W|Z^n,h_e^M,H_m^M) \tag{43}$$
$$= \int_{\mathcal{A}_M(h_e^M)} \frac{1}{n}H(W|Z^n,h_e^M,h_m^M) f_{H_m^M}(h_m^M)\,dh_m^M \tag{44}$$
$$\stackrel{(b)}{\geq} \int_{\mathcal{A}_M(h_e^M)} (R_s-\epsilon) f_{H_m^M}(h_m^M)\,dh_m^M \tag{45}$$
$$\stackrel{(c)}{=} R_s - \epsilon, \qquad \forall h_e^M \in \mathcal{E} \text{ with } P[\mathcal{E}]=1. \tag{46}$$

(a) follows from the fact that conditioning reduces the entropy, (b) follows from the fact that since $h_m^M \in \mathcal{A}_M(h_e^M)$, $(h_m^M,h_e^M) \in \mathcal{A}_M$, and (c) follows from the fact that $P[H_m \in \mathcal{A}_M(h_e^M)] = 1$.

References

[1] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[2] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[3] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels,"*IEEE Trans. Inf. Theory*,vol. 55, no. 4, pp. 1575–1590, Apr. 2009.

[4] A. D.Wyner, "The wire-tap channel". *Bell Syst. Tech. J.*, 54(8):1355–1387, October 1975

[5] T. L. Marzetta and B. M. Hochwald, "Fast transfer of channel state information in wireless systems," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1268–1278, Apr. 2006.

[6] G. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast fading channels: A block-Markov Wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, July 2012.

[7] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper,"*IEEE Trans. Signal Process.*, vol. 61, no. 1, Jan. 2013.

[8] X. Zhou, B. Maham, and A. Hjrungnes, "Pilot Contamination for Active Eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[9] Z. Rezki, A. Khisti, and M. Alouini, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, 2012, pp. 239–243.

[10] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[11] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, Compound wiretap channels, *EURASIP J. Wireless Commun. Netw.*, pp. 113, 2009, Article 142374.

[12] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan and H. EI-Gamal, "Keys through ARQ: Theory and Practice," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 737–751, Sep. 2011